PATENT APPLICATION
ATTORNEY DOCKET: 10624.0015

#12/B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Group Art Unit: 2131

MARCEL M. YUNG *ET AL* Examiner: H. Song

Serial No.: 09/429,624

Filed: October 29, 1999

Date: December 31, 2001

For: INCORPORATING SHARED
RANDOMNESS INTO DISTRIBUTED
CRYPTOGRAPHY

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
BOX CPA
Washington, D.C. 20231

Sir:

Please amend the above-identified application as follows.

IN THE CLAIMS:

Please amend claims 1-12 and 19-22, cancel claims 13 - 16 without prejudice or disclaimer, and add new claims 23-31. After amendment, claims are as follows.

1. A method of distributed cryptographic computation using a plurality of distributed electronic devices, said method comprising:

(a) computing shared values over a known and agreed context, each value being shared among a distinct subset of the plurality of distributed electronic devices;

(b) at each of a plurality of the distributed electronic devices, generating a random value using said shared values;